МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»**

Кафедра Математического и компьютерного моделирования

Исследование технологий Web3 и их применение в разработке децентрализованных приложений

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студентки 2 курса 247 группы

направление 09.04.03 — Прикладная информатика

механико-математического факультета

Мраморнова Андрея Константиновича

Научный руководитель
к.ф.-м.н., доцент С.П. Шевырев

Зав. кафедрой
зав. каф., д.ф.-м.н., доцент Ю.А. Блинков

Саратов 2023

Введение. Целью данной работы является изучение принципов разработки решений Web3, с акцентом на технологии, платформы, фреймворки и инструменты для разработки приложений. Также сравниваем подходы к разработке между различными исследованиями и отвечаем на вопросы, относящиеся к Web3 и разработке решений Web3. Демонстрируем собранных знаний происходит на примере пробного приложения.

В рамках теоретической базы рассматриваются блокчейн и технологии, связанные с блокчейном, которые лежат в основе данной работы. Затем идет развитие Web, где описывается каждая версия Web и указывается на различия между ними (Web1, Web2, Web3). В последней теоретической части рассматриваются самые распространенные решения Web3, подкрепленные примерами, а также технологии для разработки решений Web3 и выяснение того, какие технологии представляют собой полный стек Web3.

В последней части представлена реализация пробного Web3-приложения, основанного на идентифицированном стеке технологий из предыдущих глав. Описывается, какие технологии были использованы для реализации и почему были выбраны именно они. Затем представляется концепция реализации Web2-решения для того же экспериментального приложения и обсуждаются различия между ними.

Блокчейн. Популяризация блокчейна началась после 2008 года, когда неизвестный человек или группа людей под именем Сатоши Накамото изобрели криптовалюту Bitcoin. В 2009 году ее реализация была опубликована в открытом доступе как программное обеспечение с открытым исходным кодом. Биткойн - это децентрализованная криптовалюта, которая работает в одноранговой сети, где между узлами сети существует консенсус. Консенсус означает правила, по которым работает сеть блокчейн, и подтверждает достоверность информации, записанной в блоках. Сеть состоит из узлов, и их основными задачами являются:

- Определить, является ли блок транзакций легитимным, и принять или отклонить его;
- Сохранение и хранения блоков транзакций;
- Передача истории транзакций другим узлам, которым может потребоваться синхронизация с блокчейном;

Транзакции в сети проверяются узлами с помощью криптографии и записываются в публичный реестр, называемый блокчейн. Это делает транзакции между двумя участниками возможными без посредника или центрального органа. Блокчейн представляет собой последовательность блоков, в которых хранится полный список записей о транзакциях, подобно обычной финансовой книге. Каждый блок указывает на непосредственно предыдущий блок через ссылку, которая по сути является хэш-значением предыдущего блока, называемого родительским блоком.

Децентрализованное приложение или dapp - это любое приложение, которое либо само размещено в децентрализованном пространстве (например, IPFS), либо его логика зависит от децентрализованного пространства (например, блокчейн или смарт-контракты). Dapps полагаются на blockchain для обработки данных через распределенных сетей и выполнения транзакций с помощью смарт-контрактов. Подавляющее большинство dapps построено на блокчейне Ethereum, поскольку именно Ethereum популяризировал использование смарт-контрактов для приложений на блокчейне. Идеальный dapp должен быть полностью размещен в сети P2P и не нуждается в обслуживании и управлении со стороны первоначальных разработчиков.

Термин «Смарт контракт» или «Умный контракт» был введен Ником Сабо в середине 1990-х годов, который предложил перевести положения контракта в код и встроить их в программное или аппаратное обеспечение, сделав самоисполнимыми, чтобы минимизировать затраты на заключение контракта между сторонами и избежать случайных исключений или злонамеренных действий во время выполнения контракта. Умный контракт в разных дисциплинах имеет разное значение, в нашем случае он обозначает низкоуровневый код-скрипт, работающий на блокчейне.

Ethereum, запущенная в 2015 году, стала первой платформой, поддерживающей смарт-контракты (смарт-контракты рассмотрим позже). Она была построена на фундаменте Bitcoin, но с существенными отличиями. Если Bitcoin - это только платежная сеть, то Ethereum программируема, поэтому в ее сети можно создавать и внедрять смарт-контракты. В ней используется полный язык Тьюринга, позволяющий поддерживать все типы вычислений, включая циклы. Он обеспечивает абстрактный уровень, позволяющий любо-

му создавать собственные правила владения, форматы транзакций и функции перехода состояний.

Виртуальная машина Ethereum (EVM) - это среда выполнения транзакций в Ethereum (развертывание и выполнение смарт-контрактов). Она используется для прогнозирования общего состояния Ethereum для каждого блока на блокчейне по мере его добавления в цепь. Каждый узел Ethereum работает на EVM для поддержания консенсуса в блокчейне.

Узлы, на которых работает EVM, не могут предвидеть количество ресурсов, необходимых для подтверждения транзакции, что позволяет проводить атаки типа «отказ в обслуживании».

Криптокошельки - это программное приложение, используемое для просмотра баланса криптовалюты и совершения транзакций на блокчейне. Они хранят публичные и приватные ключи пользователей, предоставляя простой интерфейс для управления балансом криптовалюты.

Взаимозаменяемость — это способность актива быть взаимозаменяемым с другим идентичным активом. А токен является взаимозаменяемым, если его можно заменить другим идентичным токеном. Два разных взаимозаменяемых токена служат одной цели, даже если они разделены или обменены на другие взаимозаменяемые токены того же типа. Взаимозаменяемый токен может быть дроблен, разделен, расщеплен или обменен, и все это без изменения его стоимости.

Невзаимозаменяемый токен (NFT) определяется как криптографически уникальный, неделимый, незаменимый и проверяемый токен, который представляет данный актив, будь то цифровой или физический, на блокчейне. Уникальность вводится стандартом ERC721, где добавляется переменная uint256 под названием tokenId, и каждая пара адрес контракта и uint256 tokendId должна быть глобально уникальной.

Разработка Web. Так что такое Web3 и чем он отличается от Web2 и Web1? Интернет, вероятно, является одной из самых важных технологических революций в истории человечества, где Web, как одно из представлений Интернета, все еще находится в стадии развития. Люди часто ошибочно используют термины Интернет и Web как синонимы, хотя они имеют разные значения.

Для лучшего понимания различий между Web1, Web2 и Web3 можно посмотреть таблицу различий, в соответствии с рисунком 1.

	Web1	Web2	Web3
Назначение	Только для чтения	Чтение-запись	Чтение, запись, владение
Тип содержимого	Статический веб-контент	Динамический веб содержание	Семантическое содержание
Содержание	Главные страницы	Блоги, вики, социальные сети	Прямые трансляции, волны, цифровые активы
Владелец данных	Централизованная организация	Централизованная организация	Пользователь
Цель	Информационный обмен	Взаимодействие	Погружение
Аутентификация	Нет	Создание новых учетных записей или SSO	Связь с криптокошельком
Инфраструктура	Централизованная инфраструктура	Инфраструктура облачных вычислений, которая в основном централизованная	Децентрализованная инфраструктура
Доступность	Удобство и доступность	Удобство и доступность	Отсутствие интеграции с современными браузеры
Реклама	Баннерная реклама	Интерактивная и поведенческая реклама	Шеринг данных за вознагражде-ние
Технологии	HTML, HTTP, URL	AJAX, JavaScript, CSS3, HTML5	Блокчейн, искусственный интеллект и децентрализован-ные протоколы, AR, VR
Доход / Прибыль	Просмотры страниц	Прибыль за клик	Создание ценности

Рисунок 1 — Сравнение Web1, Web2 и Web3

Первое различие между версиями Web заключалось в их назначении. Так как Web1 был ориентирован на обмен информацией, тип контента состоял из статичных веб-страниц и предназначался только для чтения без возможности взаимодействия. Web2 был основан на динамичном веб-контенте, где целью было взаимодействие пользователей с контентом, поэтому эту версию называют Participative Social Web.

Распределенный реестр работает по заранее определенным правилам, которые согласовываются всеми участвующими узлами сети. Эти правила называются протоколом. Наиболее известным протоколом блокчейна для создания децентрализованных приложений является Ethereum, который был первым протоколом, включающим смарт-контракты.

DeFi означает децентрализованные финансы, и это был первый популярный пример решения Web3. Он представляет собой версию Web3 о более прозрачной финансовой системе с главной целью - не зависеть от регуляторов или человеческого фактора. Большинство решений DeFi позволяют пользователям управлять своими средствами в безналичной форме, используя криптокошелек.

Web3-игра - это децентрализованная версия традиционной видеоигры, в которой игрок полностью владеет своими активами и опытом, заработанными в децентрализованной экосистеме Web3-игры. Это позволяет игрокам получить инновационное преимущество - играть, чтобы зарабатывать, поскольку игровыми активами можно торговать с помощью криптовалюты.

Web3-рынок можно описать как систему, в которой набор смарт-контрактов координирует поставщиков услуг и клиентов, а также облегчает их взаимодействие. Поставщики могут предлагать множество различных уровней индивидуальных услуг или продуктов. И клиенты, и поставщики услуг будут зарабатывать один и тот же токен управления на основе их вклада в систему. Braintrust - хороший пример такого рынка.

Реализация приложения на Web3. Ранее рассматривалось различия между Web2 и Web3. Однако, стоит задача дополнительно изучить, как эти различия отражаются на разработке приложений. Для этого будет реализовано децентрализованное приложение с использованием полного стека для разработки Web3, который был представлен ранее. Стоит задача использовать хотя бы по одной технологии из каждого слоя стека, чтобы эксперимент был полноценным. Затем рассмотрим, как то же самое решение можно было бы реализовать, используя технологии полного стека Web2, как выглядела бы архитектура системы и какие технологии были бы использованы для ее реализации. Наконец, сравним наблюдаемые различия между решениями Web2 и Web3. В качестве proof-of-concept приложения будет разработано WeddingFund - децентрализованное приложение, предназначенное для сбора свадебных подарков в виде криптовалы и пожеланий на свадебных открытках. Идея решения исходит из того, что молодожены могут быть молодыми парами без больших сбережений и часто предпочитают получать деньги, а не бессмысленные подарки от приглашенных, кроме того, сама свадьба стоит

дорого, и они хотели бы позволить себе приятный медовый месяц. Предлагаемое решение позволяет пожертвовать любую сумму Эфира в созданный фонд для молодоженов, к которой должно прилагаться пожелание в виде цифровой свадебной открытки в формате изображения. Пожертвования перечисляются в фонд по смарт-контракту и могут быть собраны в любое время владельцем контракта. Пожелания свадебных открыток хранятся в децентрализованном хранилище IPFS.

Блокчейн-проводник Etherscan был использован для наблюдением за транзакциями решения в публичной тестовой сети Goerli. В соответствии с рисунком 2 можно видеть все транзакции, которые были выполнены, с соответствующими ценами на газ в транзакции. Первая транзакция, начиная с нижней, представляет собой развертывание контракта в сети, где можно понять, с какого адреса была отправлена транзакция и стоимость транзакции. Начальная стоимость контракта была равна 0. Три транзакции в середине представляют собой пожертвования в фонд, где каждое пожертвование составляло 0,001 ETH. Из этих транзакций уже можно найти адрес контракта в колонке «To». Транзакция сверху - это вывод средств, и можно заметить, что во время этой операции стоимость газа (т.е. Txn Fee) самая низкая, что объясняется тем, что для вывода средств не требуется много вычислительной мощности. Самая высокая цена газа была во время пожертвований, потому что здесь Memos был добавлен в блок.

Txns Contract Events

Block	Age	From		To	Value	Txn Fee
7728130	2 days 8 hrs ago	0xf979ec09e21b0f3907d...	IN	0x5c74e172a4c069f96ac...	0 Ether	0.00004661
7727993	2 days 9 hrs ago	0xf979ec09e21b0f3907d...	IN	0x5c74e172a4c069f96ac...	0.001 Ether	0.00029265
7727907	2 days 9 hrs ago	0xf979ec09e21b0f3907d...	IN	0x5c74e172a4c069f96ac...	0.001 Ether	0.00022215
7727867	2 days 9 hrs ago	0xf979ec09e21b0f3907d...	IN	0x5c74e172a4c069f96ac...	0.001 Ether	0.00024825
7727795	2 days 10 hrs ago	0xf979ec09e21b0f3907d...	IN	Contract Creation	0 Ether	0.0000837

Рисунок 2 — Транзакции на блоке Explorer Etherscan

Чтобы иметь возможность сравнить реализованное решение Web3 с аналогичным решением Web2, была подготовлена концепцию системной архитектуры приложения Web2. Для реализации фронтенда был выбран тот же фреймворк Next.js. При разработке Web2-решения пришлось бы дополнительно реализовать бэкенд. Для этого нужно будет использовать Node.js, а точнее Express.js, который является де-факто стандартным серверным фреймворком для Node.js. При разработке концепции решения Web2 стояла задача охватить следующие функциональные возможности:

Реализованное решение WeddingFund представляет собой полностью децентрализованное приложение, построенное на блокчейне Ethereum, основной целью которого является пожертвование средств и пожелания молодоженам в свадебной открытке.

Реализованное децентрализованное приложение было протестирован на тестовой сети Goerli. В таблице в соответствии с рисунком 3, можно увидеть стоимость каждой операции и их стоимость в Российских рублях на данный момент. Самая низкая комиссия за транзакцию была во время снятия средств, а самая высокая - во время отправки пожертвования, что вполне логично, ведь данные записывались в блок.

Операция	Цена на газ в ETH	Цена на газ в рублях (RUB)
Развертывание смарт-контракта	0.000083	12,29
Пожертвование 1	0.000248	36,72
Пожертвование 2	0.000222	32,87
Пожертвование 3	0.000292	43,24
Снятие средств	0.000046	6,81

Рисунок 3 — Цены на газ в ETH и RUB

Чтобы убедиться, что реализованное приложение действительно является Web3-приложением, было произведена его оценка его на основе принципов Web3-приложений. Приложение является децентрализованным, поскольку все данные приложения хранятся на децентрализованных объектах, где

транзакции хранятся на смарт-контракте Ethereum blockchain, а файлы изображений - на IPFS. Он также является недоверенным, поскольку не полагается на какую-либо доверенную третью сторону. Доверие распределяется между заинтересованными сторонами сети Ethereum, то есть разработчиками, майнерами и потребителями. Каждый, у кого есть криптокошелек, может участвовать в работе приложения, не требуя разрешения административных органов, поэтому оно не требует разрешений. В приложении есть встроенные платежи; пользователи делают все свои пожертвования, отправляя родную криптовалюту Ethereum - Ether. Когда сравниваются архитектуры систем Web3 и Web2, сразу становится видно, что в Web2 нет децентрализации. Если рассматривать разработанное приложение в рамках архитектуры Web2, то имеется, что каждый компонент централизован и используется централизованный внутренний сервер, и три централизованных (incloud) сервиса, а именно PayPal, Amazon S3 и Google Firebase. Разница между подходами заключается в том, что Amazon S3 централизован и контролируется Amazon, а IPFS децентрализован и контролируется пользователями. Тяжело точно определить сложность разработки решения Web2, чтобы сравнить ее со сложностью разработки решения Web3, но исходя из концепции системной архитектуры и собственного опыта разработки приложений Web2, можно отметить, что Web2 является более сложным, поскольку в нем дополнительно используется бэкенд-хранилище MySQL. Различие подходов представлено в таблице в соответствии с рисунком 4.

Подход	Web3 приложение	Web2-приложение
Фронтэнд	Next.js	Next.js
Бэкэнд	-	Node.js
Внутреннее хранилище	-	MySQL
Хранение изображений	IPFS	Amazon S3
Аутентификация	ethers.js и MetaMask	Google Firebase
Платежи	ethers.js и смарт-контракт	API PayPal

Рисунок 4 — Различие в подходах в приложениях Web3 и Web2

Заключение. Основной целью данной дипломной работы было изучение технологий для разработки решений Web3 и исследование того, какие техно-

логии в совокупности образуют полный стек для разработки Web3. Для целей исследования были изучены концепции блокчейн-технологий и Web3. Были ввели такие понятия, как Ethereum, смарт-контракты, криптокошельки, невзаимозаменяемые токены, а также газ или стоимость транзакции. Описание развития Web было продолжено, где подробно представили каждую версию Web по отдельности, а затем сравнили их, чтобы проиллюстрировать различия. Также были представлены технологии, используемые для разработки решений Web3, наиболее распространенные типы решений Web3 и примеры каждого из них. Наконец, на основе выявленных технологий, было реализовано приложение. Полученное децентрализованное приложение было назвали WeddingFund, а его целью является сбор средств для молодоженов. Сначала была представлена подготовка к практической части, где рассматривалась разработка, среда и все используемые технологии. Затем был подробно описан процесс внедрения решения и результат. Кроме того, получившееся приложение было сравнено с эквивалентной концепцией приложения Web2, чтобы легче представить различия между Web2 и Web3. В конце была разобрана возможная идеия иной реализации похожего приложения.

Вместе с тем, Web3 является технологией, которая только начинает свой путь развития. В будущем можно ожидать еще большего развития децентрализованных приложений и смарт-контрактов, а также появления новых инструментов и платформ для их разработки и использования.

Можно предположить, что в будущем Web3.0 станет неотъемлемой частью многих отраслей, включая финансовую, медиа, здравоохранение и другие.

Таким образом, можно сделать вывод, что разработка и использование Web3.0 решений имеет большое будущее, и настоящее время является хорошей возможностью для исследования и применения этих технологий в практике.